(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 August 2001 (09.08.2001)

PCT

(10) International Publication Number
WO 01/57770 A1

(51) International Patent Classification[7]: G06F 17/60, H04L 9/00

(21) International Application Number: PCT/US01/03628

(22) International Filing Date: 3 February 2001 (03.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/497,665 4 February 2000 (04.02.2000) US

(71) Applicant and
(72) Inventor: KUO, James, S. [US/US]; 5050 Xavier Common, Fremont, CA 94555 (US).

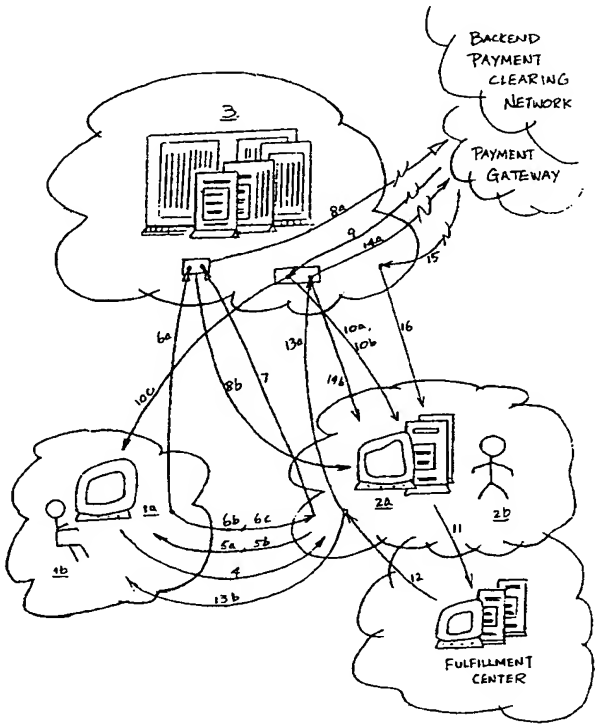
(81) Designated States *(national)*: CN, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROCESS AND METHOD FOR SECURE ONLINE TRANSACTIONS WITH CALCULATED RISK



(57) Abstract: An online method that prevents fraud due to pirated payment card numbers by utilizing SSL security techniques between a buyer (1a), a seller (2a), and a trusted payment card host (3) who has the buyers' payment card information and corresponding secret keys. The buyer (1a) initiates the transaction by utilizing a host (3) providing service to the seller's web server (2a). The buyer (1a) sends an encrypted order to the seller (2a), who assigns an order ID and sends an encrypted response to the buyer (1a) with the assigned order ID. The buyer (1a) then notifies the host (3) of this order, and authorizes the payment using secret keys. The seller (2a) sends payment approval request to the host (3). The host (3) matches up the order ID, retrieves the secret keys and hashes to obtain the corresponding payment card number. The host then requests payment authorization and notifies the seller (2a) of the card issuer's response.

WO 01/57770 A1

Patent Application of

James S. Kuo

for

TITLE: PROCESS AND METHOD FOR SECURE ONLINE TRANSACTIONS WITH CALCULATED RISK

CROSS-REFERENCE TO RELATED APPLICATIONS

Not applicable.

GOVERNMENT SPONSORSHIP

Not applicable.

MICROFICHE APPENDIX

Not applicable.

BACKGROUND - FIELD OF INVENTION

This invention relates to online transactions that take place in electronic commerce. Specifically, this invention relates to

process and method for online transactions that is relatively secure, and most importantly, it alleviates online consumer fraud that originates from pirated credit card numbers, which often occurred from online or offline sources.

BACKGROUND - DESCRIPTION OF PRIOR ART

With advent of electronic commerce, or ecommerce, the internet has brought the world together as a global trading market. Consumer at any corner of the world can buy products or services from any merchant at other parts of the world, as long as the consumer can have access to the internet and the merchant has set up a web store front. The volume of this electronic online trading is apparently huge and its growth can be explosive. What usually takes place is that, when a consumer shop at a merchant's online store, after placing an order online, the consumer will also need to enter payment information online at the that time, which is normally done by filling out a payment form that requires payment card number and certain payment card supporting information.

When merchant received the order from the consumer with payment information, the merchant will then try to fulfill the order and send in payment request to a private payment card clearing network through a payment gateway [1]. Once the merchant received the payment request response, that is payment authorization, from the payment gateway, the merchant will then deliver what the consumer ordered, and send in the request for payment capture.

This online transaction starts when the consumer entered the order with payment information, and completed when the merchant fulfilled the order and captured payment. A potential fraudulent online transaction occurs when the credit card, or payment card, that used to pay for the orders online was pirated, often from many sources. Because of the wide spread, global reach that internet enables, the potential damages to the online trading due to pirated payment cards, compared to damages it can cause to offline trading, or the traditional, old style commerce, can be many times over.

With enabling internet technologies and cryptographics algorithms today, a number of online transaction systems were proposed or developed, with varying degrees of security measures against fraud.

SET, Secure Electronic Transaction, a widely recognized, highly secure protocol for ecommerce, was first proposed by VISA, MASTERCARD, and other financial institutions in 1997[1]. Its sophisticated technological requirement has not met with wide spread deployment. Its failure in wide spread deployment should not be regarded as low acceptance among ecommerce population with respect to the importance of electronic transaction security. Rather, people have opted for other electronic transaction models that are a lot easier for merchants to deploy and for consumers to use, although they are not quite secure. That is, a user friendly, risk tolerate transaction model, which can operate without technological sophistication of the digital certificates. Set up and operate with digital certificates can be intimidating for technology novice consumers or online merchants.

Two examples of these payment devices was announced by VISA and American Express. Private Payment[12] from American Express let consumers shop using "disposable credit card numbers", instead of real credit card numbers, that can only be used once. Payer Authentication[13] from VISA, seeks to authenticate buyer by requiring additional password, when the buyer enters payment card number to place an order online. But these approaches require substantial changes to the backend payment processing protocols beyond payment gateways, especially at issuing banks' payment processors, which usually cannot take any slightest risk of error. The cost associated with deploying new or changed payment processing protocols is normally very high.

These electronic transaction models, though user friendly, are still severely compromised that they are incapable of effectively dealing with pirated payment cards, especially from online merchants point of view. Most of them do not have an effective way of blocking the usage of pirated payment card online. This shortcoming is particularly pronounced when online transaction takes place for immediate download of products or services from the merchant's web sites, where Address Verification System (AVS) is normally not applicable.

A useful and desirable electronic transaction method or protocol should be user friendly, easy to deploy, with no changes to the backend processing protocols beyond payment gateways, and at the same time, provide a sound measure against consumer fraud, which often arise from pirated payment card numbers.

SUMMARY

In an electronic commerce online transaction that prevent consumer fraud due to pirated payment card numbers, this invention involving at least one trusted payment card host. Buyer selects host, and enters order online without sending payment card number. Seller assigns an orderID to the order. Buyer authorizes payment through the host using secret keys; seller also request payment approval through the host with the same orderID. The host matches orderID and recover secret keys. The host hashes with the set of secret keys to get payment card number. The host then send payment authorization request to the payment card issuer via payment network. After receiving the response from the issuer, the host sends issuer's response back to the seller. Seller fulfills the order and send for payment capturing through the host. All messages sending and passing over the internet are SSL channel encrypted, and all messages received are decrypted by recipients.

OBJECTS AND ADVANTAGES

The objects and advantages that this invention achieved are as follows:

(1) No payment card number is used by consumers in this online transaction process, when the consumers enter orders online. Therefore, any pirated payment card, mostly from many sources, is rendered useless when a consumer is trying to use the pirated payment card number to order or shop online.

(2) It, from objects and advantages (1), provides a way to effectively

combat consumer fraud, due to pirated payment card numbers, that originates from many sources.

(3) Merchants do not handle consumer's payment card numbers in this online transaction process, it alleviates payment card abuse by fraudulent web merchants or potential dishonest employees of online merchants.

(4) It complements the existing electronic commerce practices, such as interface to internet payment gateways, or payment card clearing network, the backend payment card processors.

(5) It requires no changes beyond payment gateways. It does not require any changes to be made to the processing protocols in the backend payment clearing network, or in issuing banks' backend payment card processors.

(6) It does not restrict the device type that consumer can use to engage in online transactions, as long as the device is equipped with a web browser and plug-in ecommerce software.

(7) It does not restrict that over what kind of communication networks or communication protocols it can operate, as long as the Hosts, the Merchant Servers, and the Consumer Browsers are interconnected and can communicate with each other.

(8) It does not deliver payment card numbers over the open, unsecured network such as the internet, thus eliminates eavesdropping of payment card numbers over the internet.

(9) Based on the objects and advantages (7), this online transaction process can relief consumers' fear of shopping online simply because that they are afraid of entering payment card numbers online.

(10) This invention does not rely heavily on cryptographics. With calculated risk, it is easy to use for consumers and easy to deploy for merchants. This process and method is fairly secure with random keys, its security is not unduly compromised.

(11) With increased security measure, this invention allows frequent

changes or mutation of each set of secret keys that corresponds to each payment card account, without the need to change the underlined payment card account.

(12) It can confirm to encryption regulations of various government easily, facilitates electronic commerce deployment for global reach.

DESCRIPTION OF DRAWINGS

Fig. 1 is a schematic of an online transaction process that takes place in an electronic commerce, from the viewpoint of a participating consumer. The steps of operation flow follows numeral sequence as in this figure, from 4 to 16.

LIST OF REFERENCE OF NUMERALS

1a	consumer participant, or, buyer participant, an ecommerce device, it can be a PC computer, a handheld device, or a TV set that executes ecommerce application software
1b	the consumer, or buyer
2a	merchant participant, or, seller participant, an ecommerce application server
2b	the merchant, or seller
3	the trusted payment card host, or the host
4	consumer selects host and sends orders to the merchant participant online without including payment card number
5a	merchant participant sends order accepted response to the consumer participant with orderID
5b	merchant participant sends order-not-available response to the consumer participant
6a	consumer participant sends payment authorization request

to the host with orderID; consumer participant will optionally indicate the designations and the requirement of multiplicity of authorizations and authentications, if necessary;

6b consumer participant sends order-canceled response to the merchant participant

6c consumer participant sends payment-authorization-requested message to the merchant participant

7 merchant participant sends payment approval request to the host with orderID

8a the host retrieves all necessary secret keys from payment authorization form(s) that match the exact same orderID, then, constructs and sends transaction authorization request through payment gateways, and through payment clearing network

8b the host sends payment-approval-request-rejected response to the merchant participant

9 the host receives transaction-authorization-request response back from payment card issuer, via payment gateway or via payment clearing network

10a the host sends payment-approval-request response to the merchant participant

10b the host sends payment-approval-request-rejected response to the merchant participant

10c the host sends payment-authorization-request response to the consumer participant

11 merchant participant sends fulfillment request to the fulfillment center

12 fulfillment center sends fulfillment-request response back to the merchant participant

13a merchant participant sends payment capturing request to the host

13b merchant participant sends order-fulfilled response message to the consumer participant

14a the host sends transaction clearing request through payment gateway, or, through payment clearing network

14b the host sends payment-capturing-request-refused response back to the merchant participant

15 the host receives transaction-clearing-request response back from payment card issuer, via payment gateway, or, via payment clearing network

16 the host sends payment-capturing-request response to the merchant participant

DESCRIPTION AND OPERATION OF INVENTION - MAIN EMBODIMENT

This invention (Fig.1) provides a secure, user friendly online transaction model that alleviates consumer fraud which arises from pirated payment cards, and facilitates electronic commerce among unrestricted audience of participants, over an open, unsecured, wide area communication network, such as internet. From a localized viewpoint, that is from a single participating consumer's point of view, this electronic commerce system has a trusted payment card host (Host 3), a computer server at a participating merchant's web site (Merchant Server 2a), and a computer client at the consumer's reach (Consumer Browser 1a).

A Host 3, the trusted payment card host, is a secure computer server or servers, that hosts a repository of consumers' payment cards data. Consumers 1b register their payment cards at a Host, or at various Hosts of their choice, and set up a pair or a set of keys correspond to each payment card with the Host. For security reason, the keys are not stored in pair, but in random orders. Only the unique, correct key pair can hash out their corresponding payment card number. Each key pair, one key being authorization code, the other being authentication code are established by the payment card owner consumer with the Host. They can be changed by the owner consumer 1b at the request of the Host, or by the owner consumer self. They also can be changed at a preset periodical time, or, when deemed necessary.

A Merchant Server 2a is a computer server that merchants used to process purchase orders, and a Consumer Browser 1a is a web browser with software plug-ins that consumers used to participate in online ecommerce. Messages delivered via internet, between a Consumer Browser and a Merchant Server, between a Consumer Browser and a Host, and between a Merchant Server and a Host, are always SSL channel encrypted.

In an active ecommerce, there can be many Hosts, many Merchant Servers, and of course, many consumers, interconnected and spread over the internet, engaging in active electronic commercial transactions.

In a typical commercial transaction session, a consumer 1b initiates the online transaction by sending 4 in an order to a merchant 2b, after the consumer has done the shopping online, reviewed and confirmed the items to order. This order is delivered in a message from the Consumer Browser to the Merchant Server via internet, SSL channel encrypted. In the message, together with ordered items, are the Host of choice and an optional consumer authentication code. The selected Host is the one where the consumer has registered his or her payment card, which the consumer will use to pay for the order. The Host of choice is selected from a drop-down list of Hosts that served from the Merchant Server. This list of Hosts are those entrusted by the merchant 2b. A default trusted Host is automatically selected if no Host is chosen. The accompany authentication code corresponds to the payment card, is set up by the consumer at this selected Host 3.

Upon receiving the order, the Merchant Server 2a can check availability of ordered items, and optionally placed hold on those items for future delivery if the transaction is successfully authorized and approved. If the order cannot be fulfilled, an order-not-available response 5b will be generated and sent to the consumer, this transaction is then terminated. If the ordered items are available, in all or in part, Merchant Server will generate an orderID, and tally up the money amount for the order. Merchant Server will then generate an order accepted response 5a. The orderID and the Ordered items to be fulfilled are stored in the Merchant Server's database.

The order accepted response includes the orderID, the Host of choice

which came with original order entry, those ordered items that are available, and the money amount. This order accepted response message 5a is constructed and delivered to the consumer via internet, SSL channel encrypted. Consumer Browser receives this response and pop up a window with a payment form to be filled out by the consumer 1b. The window can be another browser window. The fields in the form includes orderID (automatically filled in already), ordered items list (already filled in), money amount (already filled in), Host of choice (already filled in, it's originally specified by consumer), consumer's payment authorization code (to be filled in), consumer authentication code (to be filled in), and other optional fields, with send and cancel buttons. Click on cancel button will abort this transaction, and an order-canceled response 6b message, which includes the orderID, will be generated and sent back to the Merchant Server that terminates this transaction. Else, after consumer filled in the blanks of the form, in accordance with the Host selected, then click on the send button, a payment authorization request 6a is generated and sent to the designated Host, and a payment-authorization-request-sent message 6c, which includes the orderID, is also generated and sent to the Merchant Server.

Upon receiving the payment-authorization-request-sent message, the Merchant Server will then construct a corresponding payment approval request 7 for this orderID, with retrieved relevant data from database of pending orders, and send it off to the selected Host.

The payment approval request 7 includes the orderID, money amount, consumer authentication code if it came with the order, and other supporting information, that are required in order to complete the processing of payment approval request. The supporting information includes merchant's financial institution, merchant ID, merchant address, etc., those data required by payment clearing network, and/or participating financial institutions to ensure that the merchant can and is legitimate to receive payment of the transaction. This payment approval request message is constructed and delivered to the Host 3 of choice, which is specified in the consumer's order entry, via internet, SSL channel encrypted.

Upon receiving Merchant Server's payment approval request, the designated Host 3, who holds the payment card data that the consumer will use to pay for

the order, will use the orderID, which is included in the payment approval request, to look up the corresponding payment authorization request 6a which has the same orderID. The Host will search inside the pool of payment authorization requests that were received within a time window around the time that the payment approval request was received. The length of this time window is determined by the Host, to reduce potential fraud, should the payment authorization request has been contaminated. In other words, this time window serves to expire the payment approval request.

If the Host 3 cannot find the payment authorization request 6a with same orderID as the payment approval request 7, within the set time window, the payment approval request is rejected, and a payment-request-rejected 8b response message with the orderID is constructed and sent back to the Merchant Server who requested it. The transaction is thus terminated.

If the Host 3 found the payment authorization request 6a with same orderID as the payment approval request 7, within the set time window, the Host will use the key pair, authorization code and authentication code that included in the payment authorization request 6a, to locate the consumer payment card data, and retrieve the payment card number. The Host will then format a transaction authorization request 8a, using the payment card number and the merchant information contained in the payment approval request 7, and send it to the consumer's payment card issuer through an Internet Payment Gateway, or other payment card clearing network.

Upon receiving the transaction-authorization-request response 9 from consumer's payment card issuer via the payment gateway, the Host 3 will determine if the issuer has approved this transaction request or not. If this request has been rejected, a payment-request-rejected response 10b message, including the orderID and the response from issuer, will be generated and sent back to the Merchant Server who requested it. The transaction is then terminated.

If the issuer approved this transaction request, the Host 3 will generate a transactionID. This transactionID includes the orderID and an approval code from issuer's response. The format of approval code may vary, depends on the payment card type or issuer. The Host stores the issuer's response 9, together with the transaction authorization request 8a under this

transactionID temporarily in Host's database, awaiting payment capturing request from the Merchant Server. The length of time before this transactionID record expires is set by the Host, it's usually more accommodating. The Host will then generate a payment-approval-request response message 10a, which includes the transactionID and send it back to the Merchant Server. The Host will also generate a payment-authorization-request 10c response message with the transactionID, and send it back to the consumer via email (since Consumer Browser may not always be up to receive Host's response).

After receiving the payment-approval-request response message 10a from the Host 3, the Merchant Server will store the transactionID in the corresponding orderID record, in the Merchant Server's database. A fulfillment request 11, which includes the orderID and those ordered items to be fulfilled, is generated and sent to the merchant's fulfillment department. The fulfillment department's computer server, upon completion of order fulfillment, will generate a fulfillmentID 12, which may include the orderID and other delivery information, and send it back to the Merchant Server.

When the Merchant Server received the fulfillmentID 12, this fulfillmentID will also be stored in the corresponding orderID record, in the Merchant Server's database. An order-fulfilled response message 13b is generated, which includes orderID and the fulfilled order items, and is sent to the consumer, via email. And a payment capturing request 13a will be generated, which includes the transactionID and money amount, and is sent back to the Host of choice 3. Upon receiving the payment capturing request 13a, the Host will verify the money amount against data stored under the transactionID. If the money amount does not match, a payment-capturing-request-refused 14b message will be generated, together with the original payment capturing request 13a, and sent back to the Merchant Server. The Merchant Server can re-transmit the payment capturing request, after receiving the payment-capturing-request-refused message, and at the same time, send an alert with the record of this orderID to the system administrator for possible offline resolution if necessary.

If the money amount and transactionID are validated by the Host, before the record expires, the Host 3 will generate a transaction clearing request

14a, which includes the consumer's payment card number, money amount, and merchant's financial data for capturing payment, and send to the payment card issuer, via an Internet Payment Gateway, or a payment card clearing network. Upon receiving the transaction-clearing-request response 15 from the consumer's payment card issuer via payment gateway, the Host 3 will generate a payment-capturing-request response message 16, which includes the transactionID, and send it back to the Merchant Server who requested it. This completes this transaction and the record of this transactionID 14a,15 is archived in the Host's archive database.

The Merchant Server will store the payment-capturing-request response message 16 in the corresponding orderID record, for future reconciliation with its financial statements from merchant's financial institution.

Consumers or merchants can query the status of financial transactions of an order or orders they requested from the Host online. The Host stores the status of the payment-authorization-request, the status of payment-approval-request, and the status of payment-capturing-request in the member accessible website which the Host has set up. The orderID can be used as the memberID for login and query, and the login password can be an email address where results of the query will be sent. The status has a timestamp, and can be either in-progress, approved with transactionID, or rejected. Consumers can also query the status of order fulfillment online at merchant's website, which the merchant has set up to be accessible to its customers.

DESCRIPTION AND OPERATION OF ALTERNATIVE EMBODIMENT

Not applicable.

CONCLUSION, RAMIFICATIONS AND SCOPE OF INVENTION

Accordingly, the reader will see several benefits of this ecommerce transaction process and method. Firstly, the consumer need not be afraid of shopping online because he or she is afraid of entering the payment card number online. In this transaction model, no payment card number is used by

the buyer when he or she shops online. In case that a payment card number has been pirated, it is rendered useless when going online within this transaction model. The fact that payment card number does not travel online will prevent eavesdropping of the payment card numbers over the internet.

Another benefit to consumers in this online transaction process is that merchant do not handle consumer's payment card number, thus it alleviates the payment card abuse by fraudulent merchants.

An additional benefit is that this transaction process can be deployed over any communication protocols or communication networks. It has a further benefit that this transaction model is also complementary to the existing payment card network systems or payment gateways, that handle authorization and settlement of payment card payments.

While my above description contains many specificities, these should not be construed as limitations on the scope of this invention, but rather as an exemplification of one preferred embodiment thereof. Many other variations are possible.

For example that in a transaction involving ordered items from multiple sellers, paid by payment cards hosted at multiple trusted payment card hosts. The same transaction process and method can equally apply, and messages to and from the buyer are encrypted and can be queued.

Another example which in order to provide buyers a gradual transition experience from current practice that buyers must enter payment card number online in order to shop, a payment card number field can also be included in the pop up payment form, in addition to secret keys fields, which is to be completed by the buyer, before it is sent off to the trusted host for payment authorization. In such a case, the host need not to hash with the secret keys to obtain the payment card number, it is readily available in the payment form to be retrieved.

Additionally, the secret keys do not have to be limited to dual pairs. For example, when a payment card account pay out must be approved by more than one party, then, each approval authority would need to have a set of

secret keys associated with that payment card account, to exercise the due power of authorization when authenticated. Authentication and authorization are verified upon submission of the secret keys.

Accordingly, the scope of this invention should be determined not only by the embodiment(s) illustrated, but by the appended claims and their legal equivalents.

TITLE: PROCESS AND METHODS FOR SECURE ONLINE TRANSACTIONS WITH CALCULATED RISK AND PROVISION AGAINST FRAUD

CLAIMS

I claim:

1. In an electronic commerce online transaction that prevent consumer fraud arises from pirated payment card numbers, involving at least one participating host, as a trusted payment card host, serving between buyers, sellers and payment clearing processors, a process and method comprising the following steps:

buyer selects a participating host, if the said host is set up as a default host, then, the selection is automatic;

buyer participant sending order for goods and services online to seller participant, without sending payment card numbers along with said order;

seller participant confirms the said order with the said buyer participant;

buyer participant authorizes the payment of the said order by sending secret keys to the said participating host; (buyer will optionally, if necessary, indicate the designations and the requirement of multiplicity of authorizations and authentications);

seller participant requests for payment approval from buyer participant's payment card issuer, through participating host;

the seller participant fulfills the said order, and requests payment capturing through the said participating host.

2. A process and method as recited in claim 1, wherein no default host is set up, the selection of participating host further comprising

the steps that the said seller participant provides a list of hosts to the said buyer participant, and the said buyer participant selects the said participating host from the said list of hosts.

2.1. A process and method as recited in claim 2, wherein the said seller participant provides a list of hosts to the said buyer participant further including steps that seller participant encrypting the said list of hosts, and buyer participant decrypting the said list of hosts.

3. A process and method as recited in claim 1, wherein buyer participant sending order for goods and services online further comprising the step of sending, alongside the said order, information of the said selected participating host.

3.1. A process and method as recited in claim 3, wherein buyer participant sending order and selected host online further comprising the steps:

the buyer participant encrypting the said order together with the said information of selected host;

the seller participant decrypts the said order and selected host.

4. A process and method as recited in claim 1, wherein seller participant confirms the said order to the said buyer participant further comprising additional steps;

seller participant generates an unique orderID that identifies the said order;

seller participant sends an independent payment form to the buyer participant for completion, wherein the said payment form includes the said orderID displayed.

4.1. A process and method as recited in claim 4, wherein the seller participant sending a payment form to buyer participant further including steps:

the seller participant encrypts the payment form;

the buyer participant decrypts the payment form.

5. A process and method as recited in claim 1, wherein buyer participant authorizes payment for the said orders further comprising additional steps:

buyer completes the said payment form by entering secret keys into pertinent spaces, the said secret keys include at least one key for authentication, and another key for authorization;

buyer participant sends the said completed payment authorization form to the said participating host;

buyer participant notify the seller participant that payment authorization form of said orderID is completed and sent.

5.1. A process and method as recited in claim 5, wherein the buyer participant sending the completed payment form to the host, further includes the steps that buyer participant encrypts the completed payment form and the participating host decrypts the said payment form.

5.2. A process and method as recited in claim 5, wherein the buyer participant notifies the seller participant further including the steps of buyer participant encrypting the message of notification, and the seller participant decrypting the said message.

6. A process and method as recited in claim 1, wherein seller participant requests for payment approval through participating host further including the steps:

seller participant encrypts the said orderID together with said payment request, and sent to the participating host;

the participating host decrypts the request.

7. A process and method as recited in claim 6, further comprising the following additional steps:

the participating host searches for all the payment authorization form(s) that matches the exact same orderID as that of the said payment approval request; (This applies to either singular or multiple authorizations and authentications);

the participating host retrieves all the necessary secret keys contained in the said payment form(s) of exact same said orderID;

the participating host hash with the said secret keys to obtain the payment card number;

the participating host sent for payment approval authorization with the said payment card number, with supporting information, through payment gateway and network.

8. A process and method as recited in claim 6, further including the following additional steps:

the participating host receives payment approval request response;

the participating host notifies the said seller participant with the said payment approval response, with orderID, but without the payment card number.

8.1 A process and method as recited in claim 8, wherein the participating host notifies the seller participant further comprising the steps:

the participating host merges the approval code, from said payment response, and the said orderID, and encrypts it and send the resulting encrypted approval response packet to the said seller participant;

the seller participant decrypts the said approval response packet and secure it in database.

9. A process and method as recited in claim 1, wherein seller participant requests payment capturing through the participating host further including the following steps:

the seller participant encrypts the payment capturing request packet, which, at least, includes the said orderID, payment approval code, and money amount, and send the resulting encrypted packet to the participating host;

the participating host decrypts the said payment capturing request packet;

the participating host verifies the payment capturing request;

the participating host send for payment capturing through payment network, with the payment card number that corresponding to the said orderID.

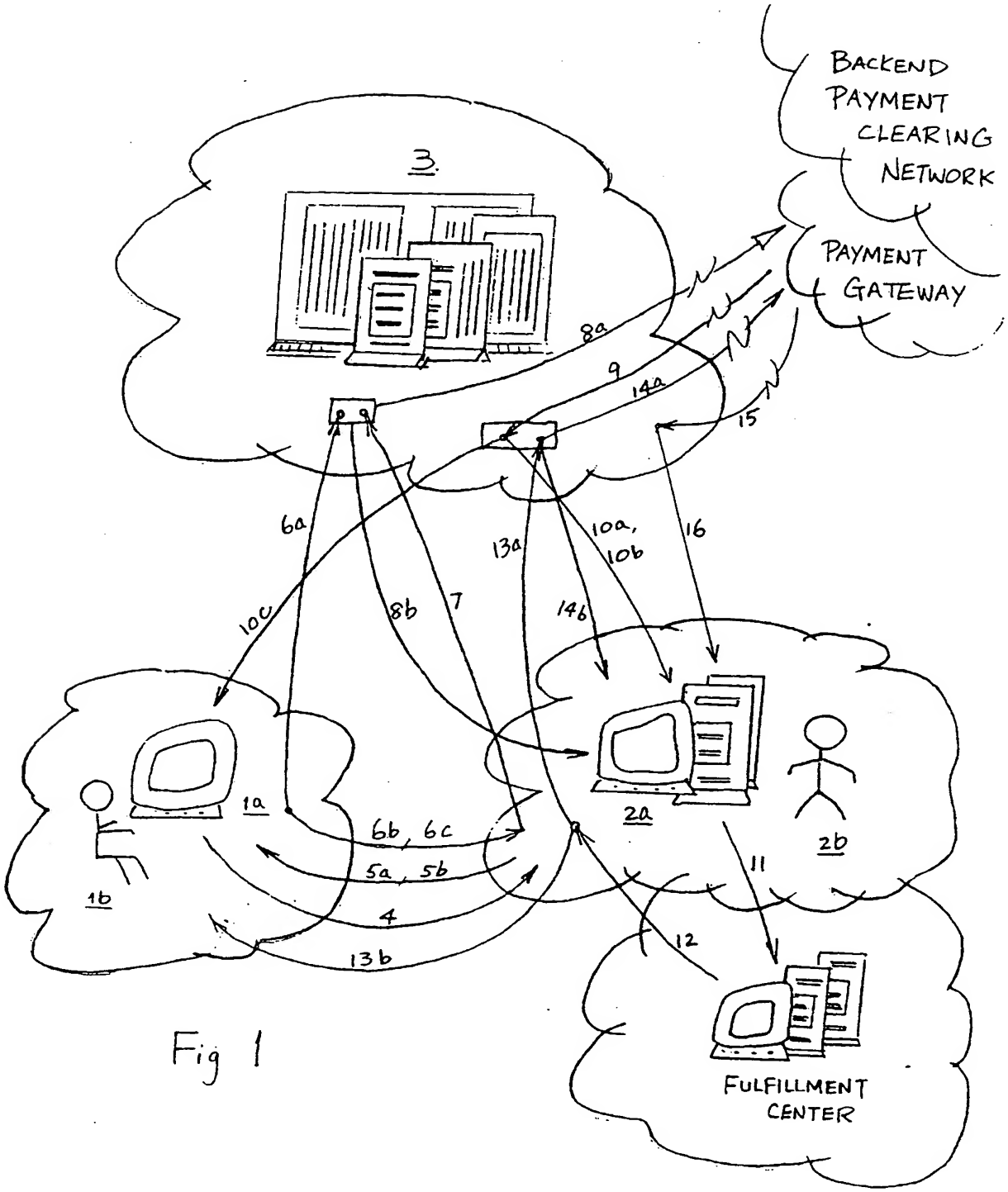


Fig 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/03628

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60; H04L 9/00
US CL : 705/1,18,26,40,44,77,80;700/232;235/379,380,382

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/1,18,26,40,44,77,80;700/232;235/379,380,382

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,794,207 A(WALKER et al) 11 August 1998 (11.08.1998), column 7, lines 43-67, column 8, lines 1-14, column 8, lines 42-44, column9, lines 60-63, column10, lines 5-8, column 12, lines 35-53, column15, lines 60-67, column 16, lines 53-63, column 21, lines 26-33, column 24, lines 24-46	1-9
Y	US 5,826,241 A (STEIN et al) 20 October 1998 (20.10.1998), column 2, lines 6-27, column 12, lines 25-64.	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 April 2001 (16.04.2001)	08 MAY 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer James P Trammell Telephone No. 703.305.3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/03628

Continuation of B. FIELDS SEARCHED Item 3: EPO;DERWENT-GO6FO17/00,GO6F01/60;
search terms: online,transactions,e-commerce,